Section 6: Use of Organization Property

6.1 Use of Equipment and Resources

Policy Statement: [Organization Name] provides various equipment and resources to its employees to facilitate the performance of their job duties. These resources include but are not limited to computers, telephones, office supplies, and vehicles. Employees are expected to use these resources responsibly and for work-related purposes only.

Procedure:

- **Authorization:** Employees must have proper authorization from their supervisor to use specific equipment and resources.
- **Care and Maintenance:** Employees are responsible for the proper care and maintenance of the equipment and resources assigned to them. Any damage or malfunction should be reported immediately to the appropriate department.
- **Personal Use:** Personal use of organization equipment and resources should be limited and should not interfere with work responsibilities. Excessive personal use may result in disciplinary action.
- **Return of Property:** Upon termination of employment, employees must return all organization property in their possession. Failure to return property may result in deductions from the final paycheck or legal action.

6.2 Technology and Internet Use

Policy Statement: [Organization Name] provides technology resources, including computers, software, email, and internet access, to enhance productivity and communication. These resources are to be used responsibly and primarily for work-related purposes.

Guidelines:

- **Acceptable Use:** Employees must use technology resources in a manner that is ethical, lawful, and consistent with the organization's policies. Acceptable use includes conducting organization business, communicating with colleagues and stakeholders, and accessing work-related information.
- **Prohibited Use:** The following activities are prohibited.
  - Accessing, downloading, or distributing inappropriate or offensive material
  - Engaging in illegal activities
  - Using technology resources for personal gain or commercial purposes
  - Sending or forwarding chain letters, spam, or other unauthorized mass communications

- **Email Etiquette:** Employees should use professional language and maintain confidentiality when sending emails. Personal opinions should be clearly stated as such and should not be represented as the organization's views.
- **Monitoring:** [Organization Name] reserves the right to monitor the use of its technology resources to ensure compliance with this policy. Employees should have no expectation of privacy when using organization equipment.

Procedure:

- **Security Measures:** Employees must follow all security protocols, including using strong passwords, logging off when not in use, and reporting any security breaches.
- **Training:** Employees will receive training on acceptable use of technology and internet resources during onboarding and at regular intervals.
- **Violations:** Any violations of this policy should be reported to the employee's supervisor or the IT department. Violations may result in disciplinary action, up to and including termination.

6.3 Telecommuting

Policy Statement: [Organization Name] recognizes the benefits of telecommuting and offers flexible work arrangements for eligible employees. Telecommuting allows employees to work from a location other than the primary office.

Eligibility: Eligibility for telecommuting is determined by the nature of the job, employee performance, and organizational needs. Not all positions are suitable for telecommuting.

Procedure:

- **Approval:** Employees must obtain approval from their supervisor and Human Resources to telecommute. An agreement outlining the terms and conditions of telecommuting will be signed by the employee, supervisor, and HR.
- **Work Environment:** Telecommuting employees are responsible for maintaining a suitable work environment, including necessary equipment, internet access, and a quiet workspace free from distractions.
- **Productivity and Communication**: Telecommuting employees must maintain productivity levels and adhere to scheduled work hours. Regular communication with supervisors and team members is required to ensure seamless workflow.
- **Data Security:** Telecommuting employees must follow all data security protocols to protect confidential information. This includes using organization-approved devices, securing networks, and following guidelines for handling sensitive data.

6.4 Use of Organization Vehicles

Policy Statement: [Organization Name] provides vehicles for employees to use for work-related purposes. The use of organization vehicles is a privilege and must be handled with care and responsibility.

Guidelines:

- **Authorization:** Only authorized employees may operate organization vehicles. Authorization must be obtained from the employee's supervisor or relevant department.
- **Driver Requirements:** Employees must hold a valid driver's license, have a clean driving record, and comply with all traffic laws and regulations.
- **Vehicle Maintenance:** Employees are responsible for ensuring that the vehicle is in good condition before and after use. Any maintenance issues or damages must be reported immediately.
- **Personal Use:** Organization vehicles are to be used for work-related purposes only. Personal use of organization vehicles is prohibited unless expressly authorized.

Procedure:

- **Booking and Log:** Employees must follow the booking procedure to reserve organization vehicles. A log of vehicle use, including mileage and purpose, must be maintained.
- **Accidents**: In the event of an accident, employees must report the incident to their supervisor and the appropriate authorities immediately. A detailed accident report must be submitted.
- **Return of Vehicles:** Vehicles must be returned to the designated location promptly after use, with a full tank of fuel if required. Keys and any related documents must be returned to the appropriate department.

6.5 Telephones and Communication Devices

Policy Statement: [Organization Name] provides telephones and communication devices to facilitate effective communication. These devices are to be used primarily for work-related purposes.

Guidelines:

- **Acceptable Use:** Employees should use organization telephones and communication devices to conduct organization business, including calls, messages, and other forms of communication.
- **Personal Use:** Limited personal use is allowed, provided it does not interfere with work responsibilities. Excessive personal use may result in disciplinary action.
- **Confidentiality:** Employees must maintain the confidentiality of all communication conducted using organization devices. Sensitive information should not be discussed in public or unsecured areas.
- **Monitoring:** [Organization Name] reserves the right to monitor the use of its telephones and communication devices to ensure compliance with this policy.

Procedure:

- **Device Security:** Employees must secure their communication devices, using passwords or other security measures to prevent unauthorized access.
- **Damage or Loss:** Any damage or loss of organization devices must be reported immediately to the IT department or the relevant supervisor. Employees may be held responsible for the replacement cost in cases of negligence.
- **Return of Devices:** Upon termination of employment or when no longer needed, communication devices must be returned to the organization in good working condition.